ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Н. А. ЖИВОДРОВА

канд. юрид. наук, доц., доц. кафедры уголовного права
Пензенского государственного университета,
г. Пенза, Российская Федерация

Развитие информационной отрасли и внедрение достижение научно-технического прогресса в деятельность общества на современном этапе является одним из ключевых векторов развития любого государства.

Однако необходимо констатировать тот факт, что в настоящее время активное развитие информационных технологий влечет за собой ряд проблем, в том числе и возникновение глобальных угроз для общества и государства. Все чаще новостные сводки сообщают об участившихся случаях кибератак, мошенничеств в сети Интернете, жертвами которых становятся крупные компании, медийные личности, так и простые граждане. Подобные новости уже не удивляют граждан.

Подтверждением роста уровня такой преступности является официальная статистика МВД России. За 2023 г. было возбуждено 676951 уголовных дел (прирост по сравнению с аналогичным периодом предыдущего года составил 29,7%) совершенных с использованием информационно - телекоммуникационных технологий или в сфере компьютерной информации, из них в сети Интернет 526794 (прирост по сравнению с аналогичным периодом предыдущего года составил 38,2%) [6].

Рост объёма информации, развитие компьютерных сетей и увеличение числа пользователей информационной среды существенно повышает вероятность хищения и неправомерного использования этой информации. Преступления в сфере информационных технологий – это одна из самых глобальных проблем для большинства современных государств.

Изучение правоприменительной практики за последние несколько лет позволяет сделать вывод о том, что в организации противодействия рассматриваемых преступлениям в настоящее время имеется множество проблем и нерешённых вопросов, отрицательно сказывающихся на всем процессе противодействия преступности.

Изначально необходимо отметить ряд факторов, порождающих распространение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. К ним относят политические, экономические, социальные и иные причины. Информационную преступность порождает высокий уровень её латентности, а также отсутствие реакции на подобные преступления со стороны жертв [1].

Помимо высокой латентности, в процессе противодействия преступлениям этой категории также имеется и ряд других проблем [8, с. 96].

Первой проблемой является то, что число раскрытых уголовных дел анализируемой группы преступлений составляет менее 1/3, так в 2023 г., согласно официальным данным МВД РФ, раскрываемость составляла 26,6 % (172290). Одной из причин этого, по мнению ученых, является тот фактор, что лица, занимающиеся расследованием данного рода

преступлений, и работники судебной системы в большинстве своем не обладают специальными познаниями в области новых компьютерных технологий, что влечет ошибки в квалификации и расследовании преступлений [3, с. 107].

Еще одной проблемой противодействия преступлениям, совершенным с использованием информационных технологий, является сложность процесса доказывания по факту наличия умысла, мотива и целей преступлений.

Проблемным вопросом является наличие серьезных сложностей при получении сведений о пользователях сети Интернет, а также их адресах IP. Преступность в сфере информационных технологий в настоящее время характеризуется как транснациональная. В связи с этим можно предположить, что преступники могут находиться на территории одного государств, жертвы на территории другого, используемые сервера на территории третьего государства [2]. Исходя из изложенного, возникают определенные сложности международного сотрудничества в целях раскрытия преступлений.

Не смотря на то, что в последнее время в СМИ массово освящаются случаи совершения противоправных деяний с использованием информационно-телекоммуникационных технологий, заявления о предостережении населения от представителей органов государственной власти, уровень информационной и компьютерной грамотности населения остается низким. Преступники это прекрасно понимают, что у указанных выше лиц отсутствуют знания в этой области, и этот факт значительно облегчает путь к получению личной и финансовой информации граждан и юридических лиц. Полученная информация в дальнейшем используется в преступных целях, например, широко распространенное мошенничество, вымогательство и ряд других преступлений.

Вместе с тем, в научной литературе и высказываются точки зрения, что государственными органами на недостаточном уровне проводится разъяснительная деятельность по информированию организаций и населения о противоправности соответствующих действий, правовых последствиях их совершения и способах обеспечения информационной безопасности и защищенности их денежных средств и иного имущества от таких посягательств [7].

Исходя из вышеизложенного, можно констатировать, что для эффективного противодействия преступлениям сфере информационно-телекоммуникационных технологий или в сфере компьютерной информации в настоящее время необходимы эффективные механизмы, в том числе и функционирующие на основе международного сотрудничества.

В практику работы правоохранительных органов необходимо внедрять возможности сети Интернет и других высоких компьютерных технологий не только по выявлению и расследованию преступлений, но и по координации их деятельности. Ряд исследователей обосновывают возможность использования искусственного интеллекта [5, 7 и др.].

В настоящее время в России, действующее законодательство, не совсем отвечает потребностям борьбы с рассматриваемой группой преступлений. Ни в уголовном законе, ни в других нормативно-правовых актах нет полного понятийного аппарата по вопросам преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Эффективность борьбы с преступлениями, совершаемых с использованием информационно-телекоммуникационных технологий необходимо повышать. Исходя из цифровизации всех сфер государственной и общественной жизни, стоит отметить, что рассматриваемый вид преступности полностью искоренить не получится, т.к. вслед за развитием общества и государства, развивается и преступный мир.

Уголовно-правовую политику в сфере противодействия преступлениям, совершаемых с использованием информационно-телекоммуникационных технологий, необходимо формировать таким способом, чтобы, в первую очередь, их предупредить и предотвратить. В этой связи стоит согласиться с К.Н. Евдокимовым, что только комплексная борьба на основе правовых, организационно-управленческих, технических и криминалистических мер сможет устранить причины и условия совершения преступлений в сфере информационно-телекоммуникационных технологий или компьютерных сетей, а также минимизировать и ликвидировать общественно-опасные последствия [4, 47-48].

СПИСОК ЛИТЕРАТУРЫ

1. Бойко, О. А., Унукович, А. С. Детерминанты латентных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий / О. А. Бойко, А. С. Унукович [Электронный ресурс] // Юридический вестник Самарского университета. 2020. №3. – Режим доступа: https://cyberleninka.ru/article/n/determinanty-latentnyh-prestupleniy-sovershaemyh-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy (дата обращения: 25.10.2024).
2. Бородкина, Т. Н., Павлюк, А. В. Киберпреступления: понятие, содержание и меры противодействия / Т. Н. Бородкина, А. В. Павлюк [Электронный ресурс] // Социально-политические науки. 2018. № 1. – Режим доступа: https://cyberleninka.ru/article/n/kiberprestupleniya-ponyatie-soderzhanie-i-mery-protivodeystviya (дата обращения: 26.10.2024).
3. Добровлянина, О. В. Внедрение новых электронных технологий в уголовное судопроизводство / О. В. Добровлянина // Ex Jure. – 2019. – № 2. – С. 104–117.
4. Евдокимов, К. Н. Противодействие компьютерной преступности: теория, законодательство, практика: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: автореферат диссертации на соискание ученой степени доктора юридических наук / К. Н. Евдокимов. – М., 2022. – 73 с.
5. Минбалеев, А. В. Проблемы использования искусственного интеллекта в противодействии киберпреступности / А. В. Минбалеев [Электронный ресурс] // Вестник ЮУрГУ. Серия: Право. 2020. №4. – Режим доступа: https://cyberleninka.ru/article/n/problemy-ispolzovaniya-iskusstvennogo-intellekta-v-protivodeystvii-kiberprestupnosti (дата обращения: 25.10.2024).
6. Состояние преступности [Электронный ресурс] // Официальный сайт МВД России. – Режим доступа: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 25.10.2024).
7. Суходолов, А. П., Бычкова, А. М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции / А. П. Суходолов, А. М. Бычкова [Электронный ресурс] // Всероссийский криминологический журнал. 2018. № 6. – Режим доступа: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-protivodeystvii-prestupnosti-ee-prognozirovanii-preduprezhdenii-i-evolyutsii (дата обращения: 26.10.2024).
8. Темиралиев, Т. С., Омаров, Е. А. Проблемы противодействия преступлениям, совершенным с применением информационных систем, и пути их решения / Т. С. Темиралиев, Е. А. Омаров // Вестник Института законодательства Республики Казахстан. – 2019. – № 1(55). – С. 93–99.